ISSN 3060-4567

KOMPYUTER VA TARMOQADA KOMPYUTER XAVFSIZLIGINI TA'MINLASH USULLARI. AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH

Farg'ona davlat universiteti,
Chet tillari fakulteti, Filologiya va tillarni o'qitish yo'nalishi 1-kurs talabasi
Nurqo'ziyeva Muxlisaxon Muqimjon qizi
e-mail: nurqoziyevamukhlisa@gmail.com
*Ilmiy rahbar:**Toshboltayev Fahriddin O'rinboyevich***
Farg'ona davlat universiteti Axborot texnologiyalari kafedrasi katta o'qituvchisi (PhD)

Annotatsiya: *Ushbu maqolada hozirgi davrda asosiy muammolardan bir bo'lgan kompyuter xavfsizligiga tahdidlar va turli hujumlar haqida bo'ladi. Shu bilan birga hujumlarga qarshi antivirus dasturlar. Bunga qo'shimcha axborotlarni himoya qilishning boshqa usullari yoritib beriladi.*

Annotation: *This article discusses one of the main problems of our time — threats to computer security and various types of attacks. It also covers antivirus programs used to counter these attacks. Additionally, other methods of protecting information are highlighted.*

Аннотация: *В данной статье рассматривается одна из основных проблем нашего времени — угрозы компьютерной безопасности и различные виды атак. Также освещаются антивирусные программы, используемые для защиты от этих атак. Дополнительно рассматриваются и другие методы защиты информации.*

Kalit so'zlar: *viruslar, wormlar, troya otlari, fishing,spear fishing, ransomware, DDoS, antivirus dasturlar, tarmoq xavfsizligiga tahdidlar, sniffing, spoofing, man-in-the-middle xujumlari, port scanning, firewall, kriptografiya, shifrlash, simmetrik shifrlash, assimetrik shifrlash.*

ISSN 3060-4567

Kompyuter xavfsizligiga bo'lgan tahdidlar va hujumlar juda xilma-xildir. Bularga viruslar, wormlar, troya otlari, fishing,spear fishing, ransomware, DDoS xujumlari va boshqalar kiradi. **Viruslar** va **wormlar** kompyuterlarga zarar yetkazib,ma'lumotlarni o'g'irlashi yoki o'chirib tashlashi mumkin. **Troya otlari** foydalanuvchilarni aldab, kompyuterga zararli dasturlarni o'rnatishga qaratilgan. **Fishing** xujumlari esa shaxsiy ma'lumotlarni o'g'irlash uchun soxta elektron pochta yoki veb-saytlardan foydalanadi. **Ransomware** xujumlari kompyuterlarni bloklab, ma'lumotlarni qaytarish uchun pul talab qiladi. **DDoS** xujumlari esa serverlarni ortiqcha yuklab, ularning ishlashini to'xtatadi.

Bundan tashqari kompyuter xavfsizligiga qarshi ichi tahdidlarlar ham mavjud. Ular asosan kompaniya xodimlari tomonidan kelib chiqishi mumkin. .Masalan, xodimlar o'z vazifalarini noto'g'ri bajarishlari, xavfsizlik siyosatiga rioya qilmasliklari yoki ma'lumotlarni o’g’irlashlari mumkin. . Shuning uchun, tashqi va ichki tahdidlarga qarshi kurashish uchun kompleks xavfsizlik choralariniko'rish zarur.

Maqola boshida keltirilgan muammolarni daf etish uchun bir nechta muqobil variantlar yaratilgan. Ulardan biri bu **antivirus dasturlar**. Antivirus dasturlari kompyuterlarni viruslar, wormlar, troya otlari va boshqa zararli dasturlardan himoya qilish uchun mo'ljallangan. Antivirus dasturlari kompyuterlardagi fayllarni skanerlab, zararli dasturlarni aniqlaydi va ularni o'chirib tashlaydi yoki karantinga joylashtiradi. Antivirus dasturlari,shuningdek, real vaqtda himoya qilish xususiyatiga ega bo'lib, kompyuterga zararli dasturlar o'rnatilishining oldini oladi.

Antivirus dasturlarini tanlashda quyidagi omillarga e'tibor berish kerak: dasturning samaradorligi, real vaqtda himoya qilish xususiyati, resurslarni iste'mol qilish darajasi, foydalanish qulayligi va narxi. Eng mashhur antivirus dasturlari: **Norton, McAfee, Kaspersky, Avast, AVG** va boshqalar.

Yana bir muammollardan biri *tarmoq xavfsizligiga tahdidlardir*. Tarmoq xavfsizligi tahdidlari kompyuter xavfsizligi tahdidlariga o'xshash bo'lishi mumkin, lekin ular tarmoq orqali tarqaladi. Tarmoq xavfsizligiga bo'lgan asosiy tahdidlar: **sniffing, spoofing, man-in-the-middle xujumlari, port scanning** va boshqalar. **Sniffing** xujumlari tarmoq orqali o'tayotgan ma'lumotlarni o'g'irlashga qaratilgan.

Spoofing xujumlari soxta IPmanzillar yoki MAC-manzillaridan foydalanib, tarmoqqa kirishga urinadi**. Man-in-the-middle** xujumlari ikki tomon o'rtasida o'tirib, ma'lumotlarni o'g'irlash yoki o'zgartirishga qaratilgan. **Port scanning** xujumlari tarmoqdagi ochiq portlarni aniqlashga qaratilgan.

Tarmoq xavfsizligini ta'minlash uchun quyidagi himoya usullaridan foydalanish mumkin: ***firewall'lardan foydalanish,intrusion detection system (IDS) va intrusion prevention system (IPS) o'rnatish, virtual private network (VPN)***dan

foydalanish, *tarmoqni segmentlash, xavfsizlik siyosatini ishlab chiqish va unga rioya qilish, xodimlarni xavfsizlik bo'yicha o'qitish.*

Firewall'lar tarmoqqa kirayotgan va chiqayotgan ma'lumotlarni filtrlash orqali xavfsizlikni ta'minlaydi. IDS va IPStarmoqdagi xavfli harakatlarni aniqlab, ularni to'xtatadi. VPN shifrlangan kanal orqali tarmoqqa xavfsiz ulanishni ta'minlaydi. Tarmoqni segmentlash tarmoqni kichik qismlarga bo'lib, xujumlar tarqalishini cheklaydi. Xavfsizlik siyosati tarmoq xavfsizligini ta'minlash bo'yicha qoidalarni belgilaydi.

So’nggi muammo bu axborot xavfsizligiga tahdid. Axborotlarni himoya qilish uchun kriptografiya va shifrlash orqali himoya qilishdir.

Kriptografiya- bu ma'lumotlarni shifrlash va shifrni ochish usullarining yig'indisidir. Kriptografiya ma'lumotlarni himoya qilish, autentifikatsiya va integrityni ta'minlash uchun ishlatiladi.

Shifrlash- bu ma'lumotlarni o'qib bo'lmaydigan shaklga o'tkazish jarayonidir.

Shifrni ochish -bu shifrlangan ma'lumotlarni o'qib bo'ladigan shaklga qaytarish jarayonidir.

Shifrlash usullari juda xilma-xildir. Bularga simmetrik shifrlash, assimetrik shifrlash, I5L-HG=>J<Olar va boshqalar kiradi.

Simmetrik shifrlashda *shifrlash va shifrni ochish uchun bir xil kalit* ishlatiladi

Assimetrik shifrlashda *shifrlash va shifrni ochish uchun turli kalitlar* ishlatiladi.

%5L-HG=>J<Olar *ma'lumotlarni o'zgarmas shaklga o'tkazish* uchun ishlatiladi.

ISSN 3060-4567

Kriptografiya algoritmlari juda murakkab bo'lishi mumkin, lekin ularning **asosiy maqsadi -ma'lumotlarni himoya qilishdir**. Kriptografiya xavfsizlik sohasida muhim ro'l o'ynaydi va ko'plab sohalarda qo'llaniladi.

Axborotlarni himoya qilishning boshqa usullari ham mavjud.Bularga *fizik xavfsizlik, ma'lumotlarni zahiralash, ma'lumotlarni yo'q qilish, xavfsizlik siyosati va xodimlarni o'qitish* kiradi. Fizik xavfsizlik ma'lumotlarni saqlash joylarini va kompyuterlarni o'g'irlikdan va shikastlanishdan himoya qiladi. Ma'lumotlarni zahiralash ma'lumotlarni yo'qotish holatlarida ularni qayta tiklash imkoniyatini beradi. Ma'lumotlarni yo'q qilish keraksiz ma'lumotlarni xavfsiz tarzda o'chirishni ta'minlaydi. Xavfsizlik siyosati axborotlarni himoya qilish bo'yicha qoidalarni belgilaydi. Xodimlarni o'qitish xodimlarning xavfsizlik bo'yicha bilimini oshiradi. Axborotlarni himoya qilishning barcha usullari birgalikda ishlatilganda eng samarali bo'ladi.

FOYDALANGAN ADABIYOTLAR:

1. Stallings, William. Cryptography and Network Security: Principles and Practice. 7th Edition, Pearson, 2017.(Kriptografiya, shifrlash usullari va tarmoq xavfsizligi haqida.)

2. Tanenbaum, Andrew S., Wetherall, David J. Computer Networks. 5th Edition, Pearson, 2011.(Tarmoq tahdidlari, sniffing, spoofing va tarmoq xavfsizligi choralari haqida.)

3. Pfleeger, Charles P., Pfleeger, Shari Lawrence. Security in Computing. 5th Edition, Prentice Hall, 2015.(Kompyuter xavfsizligi tahdidlari va himoya usullari haqida.)

Online saytlar:1.Kaspersky Lab — Cybersecurity Basics: Types of Threats and Protection Veb-sayt: https://www.kaspersky.com/resource-center/threats.

2. Symantec (Norton) — Understanding Cyber Threats Veb-sayt: https://us.norton.com/internetsecurity-malware.htm.